

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11252111 A**

(43) Date of publication of application: 17 . 09 . 99

(51) Int. Cl.

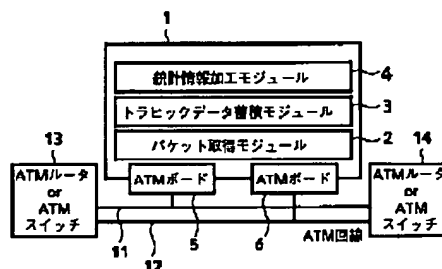
**H04L 12/28**  
**H04Q 3/00**
(21) Application number: **10053677**(22) Date of filing: **05 . 03 . 98**(71) Applicant: **KDD CORP**
(72) Inventor:  
**OGISHI TOMOHIKO**  
**IDOGAMI AKIRA**  
**KATO SATOHIKO**
(54) **TRAFFIC MONITOR DEVICE**

## (57) Abstract:

**PROBLEM TO BE SOLVED:** To compress and store traffic data in a way as close as to that of packets set through a channel for the Internet or the like.

**SOLUTION:** The traffic monitor device uses a packet acquisition module 2 to extract a packet through asynchronous transfer mode ATM lines 1, 12 of the Internet and to extract a header part including an IP header, which is given to a traffic data storage module 3. Then the module 3 checks an outgoing/incoming network ID NID of the packet and a higher-ranking protocol of the IP from the header part, records the traffic data in a preset format based on the combination between the outgoing/incoming network ID and the higher-ranking protocol according to a preset format and stores the traffic data for each prescribed time while collecting the data of the same kind of the combination. Furthermore, the traffic data storage module 3 stores the traffic data having already been stored for the same kind while collecting the data for each same kind for each prescribed longer time.

COPYRIGHT: (C)1999,JPO



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-252111

(43)公開日 平成11年(1999) 9月17日

(51)Int.Cl.<sup>8</sup>

識別記号

F I

H 0 4 L 12/28

H 0 4 L 11/20

G

H 0 4 Q 3/00

H 0 4 Q 3/00

審査請求 未請求 請求項の数12 O L (全 7 頁)

(21)出願番号 特願平10-53677

(22)出願日 平成10年(1998) 3月5日

(71)出願人 000001214

ケイディディ株式会社

東京都新宿区西新宿2丁目3番2号

(72)発明者 大岸 智彦

東京都新宿区西新宿二丁目3番2号 国際  
電信電話株式会社内

(72)発明者 井戸上 彰

東京都新宿区西新宿二丁目3番2号 国際  
電信電話株式会社内

(72)発明者 加藤 聡彦

東京都新宿区西新宿二丁目3番2号 国際  
電信電話株式会社内

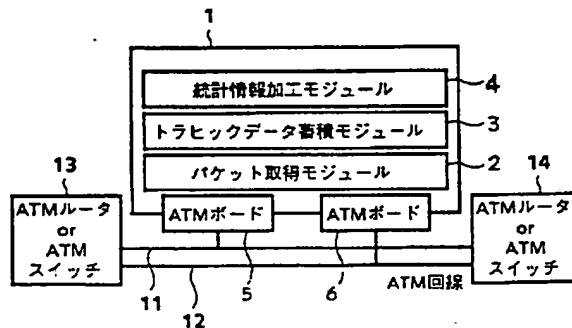
(74)代理人 弁理士 光石 俊郎 (外2名)

(54)【発明の名称】 トラヒック監視装置

(57)【要約】

【課題】 インターネット等の回線上に流れるパケットにできるだけ近い形でトラヒックデータを圧縮して蓄積すること。

【解決手段】 パケット取得モジュール2によりインターネットのATM回線1、12からパケットを抽出してIPヘッダを含むヘッダ部分を取り出し、トラヒックデータ蓄積モジュール3に渡す。モジュール3はヘッダ部分からパケットの発着NIDとIPの上位プロトコルを調べ、発着NIDと上位プロトコルの組み合わせ別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に上記組み合わせが同一種類のトラヒックデータ同士をまとめて蓄積する。更に、トラヒックデータ蓄積モジュール3により、既に同一種類毎にまとめて蓄積されたトラヒックデータ同士を、より長い一定時間毎に、同一種類毎にまとめて蓄積する。



## 【特許請求の範囲】

【請求項1】 ネットワーク間回線からパケットを抽出し、抽出したパケットの少なくともIPヘッダを含むヘッダ部分を取り出すパケット取得手段と、前記パケット取得手段が取り出したヘッダ部分の内容から同パケット取得手段が抽出したパケットのパケット発信側ネットワークID及びパケット着信側ネットワークIDとの組み合わせ（以下、発着NIDと呼ぶ）を調べ、発着NID別に、前記回線上のトラヒックに関するデータ（以下、トラヒックデータと呼ぶ）を予め設定されたフォーマットで記録し、一定時間毎に発着NIDが同一種類のトラヒックデータ同士をまとめて蓄積するトラヒックデータ蓄積手段を備えることを特徴とするトラヒック監視装置。

【請求項2】 前記トラヒックデータ蓄積手段は、発着NIDに加えて、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットのIPプロトコルよりも上位のプロトコル（以下、上位プロトコルと呼ぶ）を調べ、発着NIDと上位プロトコルの組み合わせ別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に発着NIDと上位プロトコルの組み合わせが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とする請求項1に記載のトラヒック監視装置。

【請求項3】 前記トラヒックデータ蓄積手段は、発着NIDの代わりに、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットの上位プロトコルを調べ、上位プロトコル別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に上位プロトコルが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とする請求項1に記載のトラヒック監視装置。

【請求項4】 前記上位プロトコルはTCPプロトコル、UDPプロトコル、HTTPプロトコル、FTPプロトコル及びSMTPプロトコルのうち少なくとも1つであることを特徴とする請求項2又は3に記載のトラヒック監視装置。

【請求項5】 前記トラヒックデータ蓄積手段は、前記同一種類毎にまとめて蓄積されたトラヒックデータ同士を、更に、前記一定時間より長い他の一定時間毎に、同一種類毎にまとめて蓄積することを特徴とする請求項1から4いずれかに記載のトラヒック監視装置。

【請求項6】 前記トラヒックデータとして、IPプロトコルに関する情報（以下、IP情報と呼ぶ）、TCPプロトコルに関する情報（以下、TCP情報と呼ぶ）、UDPプロトコルに関する情報（以下、UDP情報と呼ぶ）及びアプリケーションプロトコルに関する情報（以下、アプリケーションプロトコル情報と呼ぶ）のうち少なくとも1種類を含むことを特徴とする請求項1から5いずれかに記載のトラヒック監視装置。

【請求項7】 前記IP情報として、少なくともIPパケット総数及びIPパケット総バイト数を含むことを特徴とする請求項6に記載のトラヒック監視装置。

【請求項8】 前記TCP情報がコネクションに関しないTCP情報とコネクションに関するTCP情報とに区別されることを特徴とする請求項6に記載のトラヒック監視装置。

【請求項9】 前記コネクションに関しないTCP情報として少なくともTCPセグメント総数及びTCPセグメント総バイト数を含むことを特徴とする請求項8に記載のトラヒック監視装置。

【請求項10】 前記コネクションに関するTCP情報として少なくともコネクション数を含むことを特徴とする請求項8に記載のトラヒック監視装置。

【請求項11】 前記UDP情報として少なくともUDPデータグラム総数及びUDPデータグラム総バイト数を含むことを特徴とする請求項6に記載のトラヒック監視装置。

【請求項12】 前記アプリケーションプロトコル情報として、HTTPプロトコルに関する情報、FTPプロトコルに関する情報及びSMTPプロトコルに関する情報のうち少なくとも1つを含むことを特徴とする請求項6に記載のトラヒック監視装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はインターネット等、ネットワーク間のパフォーマンス解析に有用なトラヒック監視装置に関する。

【0002】

【従来の技術】インターネットの普及に伴い、特定の回線を流れるトラヒックの時間的变化など、インターネットのパフォーマンス解析が重要な課題となっている。

【0003】このようなパフォーマンス解析を行うには、回線を流れるトラヒックを長時間監視して、それに基づいて各種の統計情報を生成する必要がある。

【0004】一方、トラヒックの増大に伴い、インターネットのバックボーン回線はATM（非同期転送モード：Asynchronous Transfer Mode）回線などの使用により、高速化されてきている。

【0005】しかし、回線上に流れるパケットを加工せずに使用すると、時間に比例してデータ量が増大する。従って、ATM回線のような高速ネットワークに対してトラヒックを長時間監視する場合は、トラヒックデータの量が極めて膨大なものとなる。そのため、大容量の記憶装置と高速な処理装置が必要になる。

【0006】

【発明が解決しようとする課題】そこで本発明の課題は、回線上に流れるパケットにできるだけ近い形でトラヒックデータを圧縮して蓄積するトラヒック監視装置を提供することである。

【0007】

【課題を解決するための手段】上記課題を解決する請求項1に係る発明は、ネットワーク間回線からパケットを抽出し、抽出したパケットの少なくともIPヘッダを含むヘッダ部分を取り出すパケット取得手段と、前記パケット取得手段が取り出したヘッダ部分の内容から同パケット取得手段が抽出したパケットのパケット発信側ネットワークID及びパケット着信側ネットワークIDとの組み合わせ（以下、発着NIDと呼ぶ）を調べ、発着NID別に、前記回線上のトラヒックに関するデータ（以下、トラヒックデータと呼ぶ）を予め設定されたフォーマットで記録し、一定時間毎に発着NIDが同一種類のトラヒックデータ同士をまとめて蓄積するトラヒックデータ蓄積手段を備えることを特徴とするトラヒック監視装置である。

【0008】また、請求項2に係る発明は、前記トラヒックデータ蓄積手段が、発着NIDに加えて、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットのIPプロトコルよりも上位のプロトコル（以下、上位プロトコルと呼ぶ）を調べ、発着NIDと上位プロトコルの組み合わせ別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に発着NIDと上位プロトコルの組み合わせが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とするトラヒック監視装置である。

【0009】請求項3に係る発明は、前記トラヒックデータ蓄積手段が、発着NIDの代わりに、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットの上位プロトコルを調べ、上位プロトコル別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に上位プロトコルが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とするトラヒック監視装置である。

【0010】請求項4に係る発明は、前記上位プロトコルがTCPプロトコル、UDPプロトコル、HTTPプロトコル、FTPプロトコル及びSMTPプロトコルのうち少なくとも1つであることを特徴とするトラヒック監視装置である。

【0011】請求項5に係る発明は、前記トラヒックデータ蓄積手段が、前記同一種類毎にまとめて蓄積されたトラヒックデータ同士を、更に、前記一定時間より長い他の一定時間毎に、同一種類毎にまとめて蓄積することを特徴とするトラヒック監視装置である。

【0012】請求項6に係る発明は、前記トラヒックデータとして、IPプロトコルに関する情報（以下、IP情報と呼ぶ）、TCPプロトコルに関する情報（以下、TCP情報と呼ぶ）、UDPプロトコルに関する情報（以下、UDP情報と呼ぶ）及びアプリケーションプロトコルに関する情報（以下、アプリケーションプロトコル情報と呼ぶ）のうち少なくとも1種類を含むことを特

徴とするトラヒック監視装置である。

【0013】請求項7に係る発明は、前記IP情報として少なくともIPパケット総数及びIPパケット総バイト数を含むことを特徴とするトラヒック監視装置である。

【0014】請求項8に係る発明は、前記TCP情報がコネクションに関しないTCP情報とコネクションに関するTCP情報とに区別されることを特徴とするトラヒック監視装置である。

【0015】請求項9に係る発明は、前記コネクションに関しないTCP情報として少なくともTCPセグメント総数及びTCPセグメント総バイト数を含むことを特徴とするトラヒック監視装置である。

【0016】請求項10に係る発明は、前記コネクションに関するTCP情報として少なくともコネクション数を含むことを特徴とするトラヒック監視装置である。

【0017】請求項11に係る発明は、前記UDP情報として少なくともUDPデータグラム総数及びUDPデータグラム総バイト数を含むことを特徴とするトラヒック監視装置である。

【0018】請求項12に係る発明は、前記アプリケーションプロトコル情報として、HTTPプロトコルに関する情報、FTPプロトコルに関する情報及びSMTPプロトコルに関する情報のうち少なくとも1つを含むことを特徴とするトラヒック監視装置である。

【0019】

【発明の実施の形態】以下、本発明の実施の形態を説明する。

【0020】（トラヒック監視装置の設計方針）本発明の実施の形態に係るトラヒック監視装置の設計にあたり、以下の方針を立てた。

（1）一定時間毎（例えば、10分毎）に、IP、TCP、HTTP、FTP及びSMTP（Simple Mail Transfer Protocol：シンプルメール転送プロトコル）等の各プロトコルの統計情報を生成し、その時間的変化を解析可能とする。これらの情報は、発着ネットワークID及びアプリケーション毎に生成する。TCPでは、コネクションの確立時間や再送回数等、通信手順を考慮した情報も対象とする。

（2）インターネットのATM回線上を流れるIPパケットを取得し、一定時間のトラヒック量等を、トラヒックデータとして蓄積する。統計情報は、このデータを元に生成する。

（3）数カ月分のトラヒックデータを蓄積することを想定し、過去のデータは圧縮することが可能であるようなデータ構造を採用する。

【0021】（機能）本トラヒック監視装置には、特に、次のような統計情報を生成する機能を持たせた。

【0022】IP情報については、

（1）ATM回線を流れる総パケット数及び総バイト数

(2) 発着のネットワークID毎のパケット数及びバイト数

(3) 上位のプロトコルの種別毎のパケット数及びバイト数

等である。

【0023】TCP情報については、

(1) 確立されたコネクション数

(2) コネクションの平均接続時間

(3) コネクション当たりの平均再送パケット数

(4) コネクション当たりの平均再送バイト数

等である。

【0024】HTTP情報については、頻繁にアクセスされるサイト名等である。

【0025】(装置構成)本トラヒック監視装置は主として、CPUとソフトウェアを用いた計算機で図1に示すように構成した。但し、計算機はその能力に応じて、1台又は2台以上用いる。。

【0026】図1に示すトラヒック監視装置1は155Mbpsの第1のATM回線11及び第2のATM回線12に接続され、その上を流れる双方向のパケットを取得するように構成する。

【0027】また、図1に示すようにトラヒック監視装置1は、ソフトウェアにより、UNIXカーネル内に実装されるパケット取得モジュール(パケット取得手段)2と、ユーザプログラムとして実行されるトラヒックデータ蓄積モジュール(トラヒックデータ蓄積手段)3に加えて、データ集計及び画面表示を行う統計情報加工モジュール4から構成する。

【0028】更に、トラヒック監視装置1は、第1のATM回線11に接続するためのATMボード5と、第2のATM回線12に接続するためのATMボード6を備えている。図1中、13及び14はATM回線に接続される各ネットワークのATMルータまたはATMスイッチを示す。

【0029】(各モジュールについて)パケット取得モジュール2では、IPパケットのキャプチャを行い、IP、TCP、HTTP等のヘッダ部分を取り出し、トラヒックデータ蓄積モジュール3へ通知する。

【0030】トラヒックデータ蓄積モジュール3では、通知されたパケット情報を元に、一定時間毎にトラヒックデータを作成し、圧縮して蓄積する。

【0031】図4に、トラヒックデータのフォーマット例を示す。例えば、トラヒックデータは、一定時間内にキャプチャされた、発着ネットワークID(発着NID:発NIDと着NID)及び発着ポート(well-knownポート:発側ポート番号と着側ポート番号)が同一であるIPパケットに対して作成され、前述の統計情報を作成するための情報を保持する。

【0032】このように一定時間内に転送された複数のIPパケットに対応する情報を圧縮して蓄積することに

より、ヘッダ部分を個別に識別する場合に比べて、蓄積すべきデータ量を減少させることができると共に、過去の記録については統計情報の生成の時間間隔を長くすることにより、データの圧縮が可能である。

【0033】統計情報加工モジュール4は、蓄積されたトラヒックデータの集計及び画面表示を行う。これにより、或るネットワークIDが過去1ヶ月間にFTPにより受信したデータの総バイト数や、或るFTPサーバがTCPのコネクション確立に失敗した回数の1週間の分布など、詳細な統計情報を生成することができる。

【0034】本トラヒック監視装置1は、パケット情報を圧縮、加工して蓄積することにより、高速なインターネットに対応して長時間運用することができる。

【0035】(トラヒック監視装置1の実施例)以下、図2及び図3に基づいて、トラヒック監視装置1の具体的な実施例を説明する。

【0036】(パケット取得モジュール2の詳細)先ず、図2を参照して、パケット取得モジュール2の詳細なパケット取得処理手順を以下に説明する。

【0037】パケット取得モジュール2はATMボード5、6を通してATM回線11、12を監視し、ATM回線11、12からそこに流れるパケットを抽出してする(図2のステップS1参照)。

【0038】次に、パケット取得モジュール2は、取得したパケットからそのヘッダ部分のみを取り出す(ステップS2参照)。詳しくは、パケットのヘッダ部分からIP(インターネットプロトコル)の上位プロトコルを調べる。上位プロトコルがTCP(転送制御プロトコル:Transmission Control Protocol)及びUDP(ユーザデータグラムプロトコル:User Datagram Protocol)以外である場合は、IPヘッダのみを取り出す。上位プロトコルがTCP又はUDPである場合は、TCP又はUDPのポート番号から更に上位のアプリケーションプロトコルを調べ、アプリケーションプロトコル毎にそのフォーマットを解析して、アプリケーションプロトコルのヘッダ部分までを取り出す。

【0039】パケット取得モジュール2は、上記のように取り出したIPヘッダ及びアプリケーションプロトコルのヘッダ部分をトラヒックデータ蓄積モジュール3へ渡す(ステップS3参照)。

【0040】(トラヒックデータ蓄積モジュール3の詳細)次に、図3を参照して、トラヒックデータ蓄積モジュール3の詳細なトラヒックデータ蓄積手順を以下に説明する。

【0041】トラヒックデータ蓄積モジュール3は常時、データの圧縮を行うべき一定時間が経過したか否かを監視する(図3のステップS4参照)。

【0042】一定時間が経過しない場合は、その間、パケット取得モジュール2から渡されたデータ(IPヘッダ又はアプリケーションプロトコルのヘッダ部分)があ

るか否かを調べる（ステップS5参照）。

【0043】パケット取得モジュール2からデータが渡されていた場合は、そのデータに対応するトラフィックデータが既に存在しているか否かを調べ、そのトラフィックデータのIDを取得する（ステップS6参照）。詳しくは、パケット取得モジュール2から渡されたヘッダ部分から、パケット取得モジュール2が抽出したパケットの発着NID（発着ネットワークID）と発着ポート番号を調べることで、対応するトラフィックデータを検出し、そのIDを取得する。対応するトラフィックデータが存在していない場合は、新規にIDを付して作成する。

【0044】トラフィックデータのフォーマットとしては、発着NID及び発着ポートが同一であるIPパケットに対して作成され、大まかには、図4に符号7で示すように、IP情報、TCP情報又はUDP情報、並びに、HTTP情報という4種類の情報を記録対象とするようにしてある。

【0045】まず、トラフィックデータ蓄積モジュール3は、IP情報を記録する（ステップS7参照）。

【0046】IP情報の詳細としては、下記（1）～（6）の情報を蓄積するものとしている。

- (1) IPパケット総数
- (2) IPパケット総バイト数
- (3) パケット長の分布
- (4) IPフラグメンテーション（IPデータグラムをカプセル化する際にサイズが最大転送単位を越えた場合に分割されたIPパケット）を含むIPパケット総数
- (5) プロトコルID毎のIPパケット総数
- (6) プロトコルID毎のIPパケット総バイト数

【0047】次に、パケット取得モジュール2から渡されたヘッダ部分から、IPの上位プロトコルがTCP、UDP、それ以外（ICMP（インターネット制御メッセージプロトコル：Internet Control Message Protocol）やIGMP（インターネットグループ管理プロトコル：Internet Group Management Protocol）等）のいずれであるかを調べ、それぞれの場合について、後述のように別個の処理を行う（ステップS8参照）。

【0048】IPの上位プロトコルがTCPの場合は、まず、コネクションに関しないTCP情報を記録する（ステップS9参照）。

【0049】コネクションに関しないTCP情報の詳細としては、下記（1）～（8）の情報を蓄積するものとしている。ここで、双方向とは、サーバ側（ポート番号でアプリケーションを識別する側）からの送信と、クライアント側からの送信とを区別することを意味する。TCPセグメントのタイプとしては、SYN、SYN+ACK、DT（データセグメント）、ACK、FIN（データあり）、FIN（データ無し）、RST、これら以外の異常タイプの8つに区別する。

- (1) TCPセグメント総数（双方向）

- (2) TCPセグメント総バイト数（双方向）

- (3) MSS（最大セグメントサイズ：Maximum Segment Size）オプションを含むTCPセグメント総数（双方向）

- (4) WSF（ウィンドウスケールファクタ：Window Scale Factor）オプションを含むTCPセグメント総数（双方向）

- (5) タイムスタンプ（Time Stamp）オプションを含むTCPセグメント総数（双方向）

- (6) 再送TCPセグメント数

- (7) タイプ別のTCPセグメント総数（双方向）

- (8) タイプ別のTCPセグメント総バイト数（双方向）

【0050】次に、トラフィックデータ蓄積モジュール3は、TCPコネクションのIDを取得する（ステップS10参照）。詳細には、トラフィックデータ蓄積モジュール3はコネクション管理テーブルと状態遷移機能を備えており、抽出したパケットのTCP/IPヘッダから発着のIPアドレス及び発着のポート番号を抽出することにより、そのパケットのTCPコネクションを識別し、コネクション管理テーブルのリストから、同TCPコネクションのIDを取得する。識別したTCPコネクションがコネクション管理テーブルのリストにない場合は、当該TCPコネクションをコネクション管理テーブルに追加して新規に作成し、そのIDを取得する。

【0051】そして、トラフィックデータ蓄積モジュール3は、状態遷移及びコネクション管理テーブルの更新を行う（ステップS11参照）。詳細には、先に取得したTCPコネクションに対して、抽出したパケットのTCPヘッダを入力として与えることにより、状態遷移を行う。TCPの状態としては、CLOSED（コネクションなし）、SYN\_SENT（SYN送信済み）、ESTABLISHED（データ転送中）、INIT\_FIN\_SENT（FIN送信済み）及びRES\_FIN\_SENT（FIN受信済み）の5種類を識別するものとしている。

【0052】次に、トラフィックデータ蓄積モジュール3は、コネクションに関するTCP情報を蓄積する（ステップS12参照）。詳細には、先の状態遷移において得られるTCP情報の蓄積を行う。

【0053】コネクションに関するTCP情報としては、下記（1）～（6）の情報を蓄積するものとしている。ここでも、双方向とは、サーバ側からの送信と、クライアント側からの送信とを区別することを意味する。

- (1) TCPコネクション確立成功数
- (2) TCPコネクション確立失敗数
- (3) TCPコネクション確立平均時間
- (4) TCPコネクション持続平均時間
- (5) TCPコネクション毎の平均データ転送量（双方向）

- (6) TCPコネクション毎のスループット（双方向）

【0054】次に、トラヒックデータ蓄積モジュール3は、TCPの上位プロトコル（アプリケーションプロトコル）を調べる（ステップS13参照）。詳細には、ポート番号よりアプリケーションプロトコルを識別して、そのアプリケーション固有の情報解析を行う。

【0055】そして、TCP上のアプリケーションプロトコル毎に、そのアプリケーション固有の情報の蓄積を行う（ステップS14参照）。例えば、上位アプリケーションプロトコルがHTTP（Hyper Text Transfer Protocol：ハイパーテキスト転送プロトコル）であるならば、サイト毎のアクセス数などを蓄積する。

【0056】TCP上のアプリケーション固有の情報を蓄積したら、一定時間経過監視の処理（ステップS4）に戻る。

【0057】一方、IPの上位プロトコルの判定（ステップS8）において上位プロトコルがUDPの場合は、UDP情報を蓄積する（ステップS15参照）。

【0058】UDP情報としては下記（1）～（2）の情報を蓄積するものとしている。

（1）UDPデータグラム総数（双方向）

（2）UDPデータグラム総バイト数（双方向）

【0059】更に、トラヒックデータ蓄積モジュール3は、UDP上のアプリケーションプロトコルをポート番号より識別してそのアプリケーション固有の情報を解析し、得られたアプリケーション固有の情報の蓄積を行う（ステップS16参照）。

【0060】UDP上のアプリケーション固有の情報を蓄積したら、一定時間経過監視処理（ステップS4）に戻る。

【0061】IPの上位プロトコルの判定（ステップS8）において上位プロトコルがTCPでも、UDPでもない場合は、一定時間経過監視の処理（ステップS4）に戻る。

【0062】そして、圧縮すべき一定時間が経過した時、過去のトラヒックデータを、粒度の粗いトラヒックデータに圧縮して変換する（ステップS17参照）。

【0063】圧縮としては、発着NIDが同一種類のトラヒックデータ同士をまとめたり、発着NIDと上位プロトコル（アプリケーションプロトコルであっても良

い）が同一種類のトラヒックデータ同士をまとめたり、上位プロトコル（アプリケーションプロトコルであっても良い）が同一種類のトラヒックデータ同士をまとめて蓄積することにより、達成できる。

【0064】同一種類毎にまとめて圧縮されたトラヒックデータ同士を、より長い一定時間毎に、更に同一種類毎にまとめて圧縮して蓄積することにより、粒度がより粗いトラヒックデータに圧縮しても良い。もちろん、必要に応じて何段階にも時間間隔を長くして次々に粒度が粗いトラヒックデータに圧縮しても良い。

【0065】上記説明では、トラヒック監視装置1がインターネット中のATM回線に接続されているが、ATM回線以外の回線に接続されても良く、更には、インターネットに限らず、任意のネットワーク間の回線に接続されても良い。

【0066】

【発明の効果】以上より、本発明によれば、ネットワーク間の回線上に流れるパケットにできるだけ近い形でトラヒックデータを圧縮して蓄積することができる。従って、高速なインターネット等に対応して、トラヒック監視を長時間運用すること事ができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るトラヒック監視装置の構成例を示す図。

【図2】パケット取得手段の処理手順例を示す図。

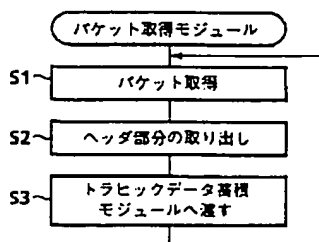
【図3】トラヒックデータ蓄積手段の処理手順例を示す図。

【図4】トラヒックデータのフォーマット例を示す図。

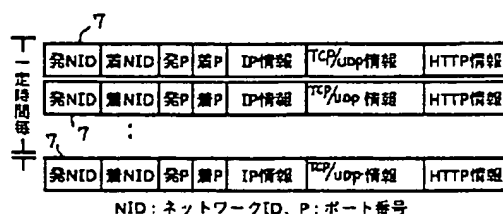
【符号の説明】

- 1 トラヒック監視装置
- 2 パケット取得モジュール（パケット取得手段）
- 3 トラヒックデータ蓄積モジュール（トラヒックデータ蓄積手段）
- 4 統計情報加工モジュール
- 5、6 ATM回線
- 7 トラヒックデータフォーマット
- 11、12 ATMボード
- 13、14 ATMルータ又はATMスイッチ

【図2】

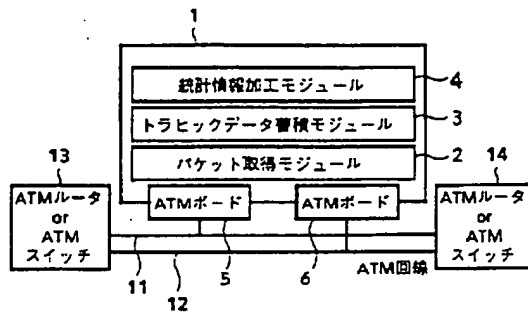


【図4】





【図1】



【図3】

